



Digitalization and its Impact on Non-Banking Financial Companies: Barriers, Enablers, and Strategic Implications

Saurav Dhar¹; Dipak Jain¹; Saket Jeswani²

¹Royal School of Business, The Assam Royal Global University, Guwahati, India

²Faculty of Commerce and Management, Kalinga University, Raipur, Chhattisgarh, India

Corresponding Email: djain@rgi.edu.in

Article History:

Received: February 11, 2025

Accepted: April 7, 2025

Online First: June 30, 2025

Keywords:

non-banking financial companies; digitalization; artificial intelligence; robotic process automation; cybersecurity; technology adoption; financial inclusion; India

This is an open access article under the CC-BY-NC-ND license.



Abstract: The digitalization of financial services has repositioned Non-Banking Financial Companies (NBFCs) as a critically important yet structurally vulnerable constituency of India's financial ecosystem. As technologies including Artificial Intelligence (AI), Robotic Process Automation (RPA), and advanced cybersecurity systems become operationally indispensable, the capacity of NBFCs to adopt these tools efficiently and safely has become a material determinant of their institutional survival and competitive relevance. This study examines the adoption barriers, operational challenges, and measurable benefits of technology integration among NBFCs registered in Guwahati, Assam, using primary survey data collected from forty institutional respondents through a semi-structured questionnaire administered in 2024. Analysis reveals that workforce skill deficits (45.2%) and technology acquisition costs (35.7%) constitute the primary structural barriers to adoption, while system compatibility challenges (59.5%) emerge as the dominant technical obstacle. Regulatory compliance, whilst present as a challenge, is perceived by the majority of institutions as only slightly challenging (73.8%), with financial reporting requirements generating the greatest procedural difficulty (45.2%). Data security breaches are identified as the foremost long-term institutional risk (71.4%), a finding that aligns with national-level evidence of intensifying cybersecurity threats in India's Banking, Financial Services, and Insurance sector. Despite these constraints, AI is broadly perceived as effective in enhancing decision-making, RPA is adopted primarily for the automation of high-volume repetitive processes, and vendor technical support is rated favorably by over 83% of respondents. The study concludes with recommendations for institutional capacity-building, strategic technology investment, and regulatory navigation frameworks adapted to the resource constraints characteristic of smaller NBFC institutions.

How to cite:

Shalini, R., & Yuvashree, M. (2025). Digitalization and its impact on non-banking financial companies: Barriers, enablers, and strategic implications. *Business and Organization Studies e-Journal*, 3(2), 24-46.



INTRODUCTION

India's financial architecture has undergone a sustained structural transformation since the liberalization period, with Non-Banking Financial Companies (NBFCs) progressively occupying an intermediation role that the formal banking sector, bound by stricter regulatory constraints and collateral requirements, has been structurally ill-positioned to fulfil. NBFCs serve the credit needs of micro, small, and medium enterprises, agricultural households, informal sector workers, and first-generation borrowers whose financial profiles fall outside the risk appetite of conventional deposit-taking institutions. The breadth and depth of this intermediation function is substantial: by 2023, the NBFC sector contributed approximately 12.6% of India's gross domestic product and held a market share of nearly 30% of the country's total non-food credit – a share that has grown consistently over the preceding five years, encroaching on territory once regarded as the exclusive domain of scheduled commercial banks (Elets BFSI, 2024).

The digitalization of financial services has simultaneously created new opportunities and new institutional challenges for NBFCs. On the opportunity side, the proliferation of mobile-first digital infrastructure, the expansion of India's data economy, and the emergence of Account Aggregator frameworks, the Open Credit Enablement Network, and Open Network for Digital Commerce have generated the technical preconditions for NBFC products to reach previously unserved consumer segments at scale and with commercially viable unit economics (Elets BFSI, 2024). On the challenge side, the same digital infrastructure has expanded the cybersecurity threat surface of institutions that often possess leaner technology and compliance teams than their banking counterparts, while simultaneously increasing the regulatory complexity of operating in an environment characterized by rapidly evolving data protection requirements and technology-specific oversight frameworks. The Reserve Bank of India's Master Direction on IT Governance, Risk, Controls, and Assurance (2023) has significantly raised the institutional baseline for technology governance across all regulated financial entities, including NBFCs, adding to the compliance burden that technology adoption already entails.

Academic research on NBFC digitalization has grown in volume over the past decade, reflecting the sector's growing systemic importance. Studies have examined credit risk assessment using machine learning (Manukyan & Parsyan, 2024; Edunjobi & Odejide, 2024), the operational efficiency gains generated by RPA implementation (Jangir et al., 2024), the role of NBFCs in MSME financing (Shah, 2023), and the dynamics of customer relationship management under digital transformation (Khan, 2023). However, primary empirical evidence on how NBFCs in Tier-2 and Tier-3 Indian cities – which face resource constraints not reflected in studies conducted in metropolitan financial centers – are experiencing, perceiving, and navigating the



barriers and benefits of technology adoption remains limited. This study addresses that gap by examining digitalization challenges and outcomes at the institutional level among NBFCs registered in Guwahati, Assam, a northeastern Indian city whose NBFC population is geographically and institutionally distinct from the Mumbai-Bengaluru corridor that dominates the existing literature.

This paper is organized as follows. Section 2 reviews the relevant theoretical and empirical literature. Section 3 describes the research methodology, including data sources, sample characteristics, and analytical procedures. Section 4 presents the survey findings across fourteen analytical dimensions. Section 5 discusses the implications of the findings. Section 6 concludes with strategic recommendations and directions for future research.

LITERATURE REVIEW

NBFCs in India: Growth, Role, and Structural Characteristics

The regulatory and operational architecture of NBFCs distinguishes them from scheduled commercial banks in ways that are directly relevant to their technology adoption profiles. Whilst banks are licensed to accept demand deposits and are subject to the full scope of the Reserve Bank of India's prudential framework, NBFCs derive funding primarily from market borrowings, debentures, and fixed deposits in formats governed by a separate and somewhat lighter regulatory regime. This structural difference has historically enabled NBFCs to innovate in product design and credit delivery more rapidly than banks, but it has also left them more exposed to liquidity risk and less capable of absorbing the compliance and technology investment costs that the current phase of digital regulatory expansion demands (Sengupta, Son, & Vardhan, 2022). Kaur (2019) documented the growth trajectory of NBFCs through the mid-2010s, identifying regulatory liberalization, financial inclusion imperatives, and digital connectivity as the primary drivers of sector expansion. Shah (2023) extended this analysis to the MSME credit segment, demonstrating that NBFCs have become indispensable intermediaries for small business financing in regions and sectors where formal bank credit remains structurally constrained.

Artificial Intelligence in Financial Services

The application of artificial intelligence to financial services has been one of the most extensively studied phenomena in the financial technology literature over the past decade. AI technologies — encompassing machine learning, natural language processing, computer vision, and predictive analytics — have demonstrated measurable performance gains across multiple NBFC-relevant applications: credit



underwriting, fraud detection, customer onboarding, portfolio monitoring, and regulatory reporting (Manukyan & Parsyan, 2024). Edunjobi and Odejide (2024) provided a systematic review of AI-driven credit risk assessment frameworks, demonstrating that machine learning-based models consistently outperform traditional scoring approaches on discrimination accuracy and calibration quality, particularly for thin-file borrowers whose credit histories are insufficient for conventional scorecard models – precisely the demographic that constitutes the core NBFC customer base. Chen, Wu, and Zhang (2023), writing in *Technological Forecasting and Social Change*, established a direct positive relationship between AI adoption intensity and financial innovation performance in emerging market financial institutions, arguing that AI's most material contribution lies not in cost reduction but in the expansion of the addressable market through more sophisticated risk segmentation.

The Indian NBFC sector's engagement with AI, whilst growing, has been uneven across institution size and geography. Larger NBFCs and those operating in metropolitan markets have deployed AI-powered chatbots, digital know-your-customer solutions, and automated collections systems at scale. Smaller and geographically dispersed NBFCs – including those in northeastern India that constitute this study's sample – have been slower to adopt, constrained by technology acquisition costs, the scarcity of data science talent in their operating territories, and the absence of AI-specific regulatory guidance from the RBI that would reduce adoption uncertainty (Jangir et al., 2024). The result is a technology adoption gradient within the NBFC sector that mirrors and risks reinforcing existing institutional hierarchies.

Robotic Process Automation: Efficiency Gains and Implementation Barriers

Robotic Process Automation has attracted growing scholarly and practitioner interest as a complement to AI in the financial services digitalization agenda. Unlike AI systems that learn from data and improve their outputs through feedback, RPA software executes predefined rule-based processes at machine speed, interfacing with existing applications through their user interfaces without requiring changes to underlying system architecture. This characteristic makes RPA particularly attractive to NBFCs because it allows automation benefits to be realized without the deep system integration that full digital transformation would require – a critical advantage for institutions constrained by legacy IT infrastructure (Mamede, Gonçalves Martins, & Mira da Silva, 2023). Jangir et al. (2024) demonstrated, through an empirical study of RPA adoption among Indian NBFCs, that the technology generated significant reductions in processing time, error rates, and compliance documentation costs in the functions where it was deployed, with back-office transaction reconciliation and regulatory report generation identified as the highest-



value automation targets. The RPA market in the financial services sector is projected to exceed USD 13 billion globally by 2030, with Indian financial institutions accounting for a growing share of adoption as digital-first business models proliferate.

The implementation of RPA is not, however, without institutional challenges. System compatibility – the ability to interface RPA software with existing core banking, loan management, and customer relationship platforms – emerges consistently in the empirical literature as the primary technical barrier to successful deployment. Mamede et al. (2023), in a study of RPA adoption at a private bank in Portugal, demonstrated that applying Lean process-improvement techniques before RPA deployment – effectively simplifying and standardizing the processes to be automated before automation is introduced – produced substantially greater efficiency gains than direct RPA implementation on existing, unstructured processes. This finding has implications for the sequence of institutional investments that NBFCs should contemplate in their technology roadmaps.

Cybersecurity in the Digital Financial Services Environment

The expansion of digital financial services has been accompanied by a commensurate intensification of cybersecurity threats targeting financial institutions. India's BFSI sector has experienced a particularly sharp increase in cyber incident frequency and sophistication: CERT-In recorded 4,29,847 cybersecurity incidents pertaining to financial institutions in 2023, representing a dramatic increase from 6,168 in 2019 and confirming the assessment of India's Digital Threat Report 2024 that the financial sector's rapid digital transformation has materially expanded its attack surface (PwC India, 2024). The average cost of a data breach for Indian financial enterprises reached USD 2.35 million in 2024, an increase of 7.8% year-on-year, substantially below the global financial sector average of USD 6.08 million but nevertheless a material operational risk for smaller NBFCs operating on thin capital buffers (IBM, 2024, as cited in Fintech News Singapore, 2025). The 2024 Digital Threat Report – jointly published by CERT-In, CSIRT-Fin, and cybersecurity firm SISA – identified AI-driven phishing campaigns, ransomware, third-party supply chain vulnerabilities, and deepfake-enabled identity fraud as the four primary emerging threats facing India's financial sector in the near term (CERT-In, CSIRT-Fin & SISA, 2024).

NBFCs are structurally more exposed to these threats than banks for a predictable reason: their digital-first operating models and large repositories of customer financial and identity data make them high-value targets for cybercriminals, whilst their typically leaner security teams and smaller cybersecurity budgets relative to their data custody responsibilities create an unfavorable security equation that is



difficult to resolve without structural investment (Elets BFSI, 2026). Rai et al. (2023), in an analysis of the intersection of financial technology and cybersecurity in India, documented the increasing sophistication of attacks targeting NBFC-scale institutions and argued that encryption, AI-driven anomaly detection, and multi-factor authentication are no longer optional security enhancements but baseline requirements for regulatory compliance and institutional viability under the Digital Personal Data Protection Act, 2023.

Regulatory Compliance and Digital Governance

The regulatory environment governing NBFC technology adoption in India has grown considerably more complex over the period covered by this study. The RBI's Master Direction on IT Governance, Risk, Controls, and Assurance (2023) established comprehensive new requirements for IT governance structures, risk management systems, business continuity planning, and internal audit functions for all regulated entities, including NBFCs. These requirements, while necessary from a systemic stability perspective, impose institutional overheads that are disproportionately challenging for smaller NBFCs whose compliance functions are not resourced to manage simultaneous obligations under multiple regulatory frameworks. Ahmed (2024), in a comparative analysis of non-banking financial institutions in Bangladesh, documented analogous dynamics in a neighboring emerging market context, finding that regulatory compliance costs constituted the single largest non-core operational expense for technology-adopting institutions, and that smaller institutions bore compliance cost burdens that were proportionally higher than their larger counterparts. Loutfi (2022), examining the business deployability of digital footprint-based credit models, identified data privacy compliance – specifically, the need to reconcile commercial use of customer data with the evolving requirements of data protection regulation – as the most durable structural challenge facing financial institutions deploying AI-based credit assessment at scale.

RESEARCH METHODOLOGY

Research Design and Data Sources

This study adopts a descriptive quantitative research design to characterize the current state of advanced technology adoption among NBFCs in Guwahati, Assam, and to identify the institutional challenges and perceived benefits associated with that adoption. Descriptive research is appropriate for this study's objectives because it aims to produce a systematic, empirically grounded characterization of adoption



patterns and institutional experiences without manipulating or controlling the variables under examination.

Primary data were collected through a semi-structured questionnaire administered to institutional representatives of NBFCs registered with the Reserve Bank of India in Guwahati City during the 2024 fiscal year. Secondary data, used to contextualize findings, were drawn from published reports, regulatory circulars, and peer-reviewed studies.

Population and Sample

The target population comprised all 60 non-banking financial companies registered in Guwahati City as of the date of data collection. Of these 60 institutions, 20 were registered in Guwahati but maintained their principal operations in other states, rendering in-person or institutional survey participation logistically infeasible. The effective survey population was therefore 40 institutions, all of which were contacted and invited to participate. All 40 institutions provided usable responses, yielding a 100% response rate within the accessible population.

Given the non-probability character of the sample – determined entirely by geographic accessibility rather than random selection from the full national population of NBFCs – the findings should be interpreted as representative of NBFCs in the Guwahati operating environment and generalizable with caution to comparable Tier-2 northeastern Indian city contexts. They are not directly generalizable to metropolitan NBFC ecosystems such as Mumbai, Bengaluru, or Hyderabad, where institutional characteristics, IT infrastructure, and talent availability differ substantially.

Instrument and Procedures

The questionnaire comprised fourteen thematic survey items covering: the primary challenges of advanced technology implementation; the perceived ease of technology-legacy system integration; the principal sources of internal resistance to technology adoption; the intensity and character of regulatory compliance challenges; the most demanding specific regulatory dimensions; the frequency of regulatory change impacts; the predominant technical obstacles to deployment; the quality of vendor technical support; the priority areas for technology feature improvement; the most notable long-term technology benefits; the preferred success metrics for technology implementations; the most significant long-term technology adoption risks; the areas of most acute need for practical guidance; and the adequacy of currently available implementation guidance. Responses were collected using a mix of single-response and multiple-response categorical formats, enabling frequency and proportional analysis of each dimension.



RESULTS AND DISCUSSION

Primary Challenges of Advanced Technology Implementation

The distribution of implementation challenges reveals a workforce-centered rather than technology-centered primary barrier. Nearly half of responding institutions (45.2%) identified the lack of skilled personnel as their foremost implementation challenge – a finding that accords with the broader pattern of AI and technology adoption barriers documented in developing financial markets, where the supply of trained data scientists, AI architects, and cybersecurity specialists consistently lags demand from the financial services sector (Jangir et al., 2024). The technology cost barrier, identified by 35.7% of respondents, represents the second most pressing concern. These two findings are structurally related: smaller NBFCs face a compounding disadvantage in which high technology acquisition costs foreclose the option of in-house system development, whilst the cost of hiring or contracting specialized technology talent – which represents the alternative pathway to digital capability – is similarly prohibitive on their budget envelopes. Regulatory compliance, despite its prominence in the scholarly and policy discourse on NBFC digitalization, was identified as a primary implementation challenge by only 2.4% of respondents. This apparent underweighting is contextualized by the findings on regulatory compliance intensity, and likely reflects the framing of the question: regulatory compliance is a pervasive ambient challenge rather than a discrete implementation barrier for most institutions in the sample.

Table 1.
Primary Challenges of Advanced Technology Implementation (N = 42)*

Challenge Category	n	(%)
High cost of technology	15	35.7
Lack of skilled personnel	19	45.2
Integration with existing systems	7	16.7
Regulatory compliance	1	2.4

Note. *Discrepancy between n and sample size reflects multiple-response options or institutional-level aggregation.



Ease of Integrating New Technologies with Existing Systems

The integration difficulty ratings describe a distribution that is concentrated around the neutral and moderately positive range, with only 21.4% of respondents describing integration as difficult or very difficult and 38.1% describing it as easy or very easy. This distribution pattern – which is essentially symmetric about the neutral midpoint – suggests that the integration challenge, whilst real, is not perceived as an existential obstacle for most institutions in the sample. The modal response of 'Neutral' (40.5%) is consistent with the finding that system compatibility is the primary technical obstacle to technology deployment: compatibility concerns may generate friction and transition costs without necessarily preventing implementation, explaining why many respondents occupy the neutral rather than the negative end of the scale. The finding that only 2.4% of respondents rate integration as 'Very Difficult' suggests that the middleware, API, and vendor-facilitated integration tools available to these institutions are sufficiently functional to manage the integration task, even if imperfectly. This contrasts with the perception in some NBFC policy discourse that legacy system integration represents a categorical barrier to digital transformation, and it suggests that targeted investment in integration tooling could efficiently move the modal institutional experience from neutral to positive.

Table 2.
Ease of Integrating New Technologies with Existing Systems (N = 42)

Rating	n	(%)
Very Easy	1	2.4
Somewhat Easy	15	35.7
Neutral	17	40.5
Somewhat Difficult	8	19.0
Very Difficult	1	2.4

Primary Sources of Resistance to Technology Adoption

Employee resistance is identified as the primary source of adoption resistance by 42.9% of respondents – a finding whose institutional significance extends well beyond the immediate technology implementation context. Employee resistance to



technology adoption in financial services institutions typically reflects a combination of perceived threat to existing roles, skill inadequacy relative to the demands of new systems, and insufficient institutional support for the transition process. The finding that employee resistance substantially exceeds management resistance (9.5%) as a reported barrier indicates that the institutional leadership of the sampled NBFCs is, in principle, committed to technology adoption but may be underinvesting in the workforce development and change management interventions necessary to bring operational staff along with the transformation agenda. This interpretation is reinforced by the finding that 'training and support' was among the most frequently cited areas of acute need for practical guidance.

Table 3.
Primary Sources of Resistance to Technology Adoption (N = 42)

Source of Resistance	n	(%)
Lack of management support	4	9.5
Employee resistance	18	42.9
Technical difficulties	13	31.0
Cost concerns	7	16.7

Technical difficulties as a resistance source (31.0%) capture the combined effect of insufficient IT infrastructure, vendor support limitations, and skill deficits in managing the technology itself – a category of resistance that is distinct from the human-centered resistance that employee pushback represents and that responds to different intervention types. Cost concerns (16.7%) represent the smallest identified resistance category, consistent with the finding that institutional leadership, which bears budget allocation responsibility, is less resistant to adoption than the employees who must implement it.

Intensity of Regulatory Compliance Challenges

The distribution of regulatory compliance challenge intensity is notable both for what it shows and for what it implies about the institutional relationship between NBFCs and their regulatory environment. Nearly three-quarters of respondents (73.8%) describe regulatory compliance during technology implementation as 'slightly challenging' – a characterization that implies the regulatory environment is



present as an institutional consideration without being operationally disabling. Only one respondent (2.4%) characterized it as 'very challenging.' This finding should be interpreted with some caution: the 'slightly challenging' modal response may reflect the normalization of regulatory complexity among experienced NBFC professionals who have developed institutional routines for managing compliance, rather than indicating that the compliance burden is genuinely light. It may also reflect the sample's preponderance of smaller NBFCs undertaking relatively early-stage technology adoption, where the compliance implications are less complex than those confronting institutions at later stages of digital transformation.

Table 4.

Degree of Challenge in Regulatory Compliance during Technology Implementation (N = 42)

Challenge Level	n	(%)
Not challenging at all	2	4.8
Slightly challenging	31	73.8
Moderately challenging	8	19.0
Very challenging	1	2.4

Most Challenging Specific Regulatory Dimensions

Financial reporting requirements emerge as the most challenging specific regulatory dimension (45.2%), a finding consistent with the substantial impact that technology system changes have on the data extraction, transformation, and reporting pipelines that NBFCs must maintain for RBI and SEBI regulatory reporting. When a new technology system is introduced, the mapping of transactional data to regulatory reporting templates must be reconfigured and validated, a process that is technically demanding, time-sensitive, and consequential for institutional compliance standing. Data privacy laws and technology-specific regulations are each identified as most challenging by 19.0% of respondents. The prominence of data privacy law as a compliance challenge reflects the regulatory transition underway in India following the enactment of the Digital Personal Data Protection Act, 2023, which has introduced new consent requirements, data localization obligations, and breach notification



standards that add compliance dimensions to every technology system that processes customer personal data (Rai et al., 2023).

Table 5.
Most Challenging Regulatory Aspect in Technology Deployment (N = 42)

Regulatory Aspect	n	(%)
Data privacy laws	8	19.0
Financial reporting requirements	19	45.2
Anti-money laundering regulations	7	16.7
Technology-specific regulations	8	19.0

Frequency of Regulatory Change Impacts

Half of respondents (50.0%) report that regulatory changes 'sometimes' impact their technology implementation processes, whilst 41.8% report that they do so 'often' or 'always.' Only 7.2% report that regulatory changes rarely or never affect their implementation trajectory. Collectively, these figures establish that regulatory change is a material and recurring feature of the technology adoption landscape for the vast

Table 6.
Frequency of Regulatory Changes Impacting Technology Implementation (N = 42)

Frequency	n	(%)
Always	4	9.5
Often	14	32.3
Sometimes	21	50.0
Rarely	2	4.8
Never	1	2.4



majority of institutions in the sample – one that institutions must anticipate and accommodate in their technology roadmaps rather than treating as an occasional exogenous disruption. The practical implication is that technology adoption plans must incorporate regulatory monitoring and change-management processes as first-order institutional functions, not afterthoughts. The RBI's demonstrated pattern of iterative and sometimes rapid regulatory evolution in the technology governance space – exemplified by the progression from the Cyber Security Framework of 2016 through the Master Direction on IT Governance, Risk, Controls, and Assurance of 2023 – suggests that this regulatory dynamism will persist rather than stabilize.

Key Technical Issues Impacting Technology Deployment

System compatibility is identified as the dominant technical obstacle to technology deployment by an overwhelming majority of respondents (59.5%), establishing it as the single most operationally significant technical constraint in this sample. The system compatibility challenge for NBFCs has a specific and well-documented character: core lending management systems, accounting platforms, and customer data environments in smaller financial institutions are frequently legacy systems operating on software architectures that predate modern API standards, making the integration of AI modules, RPA bots, and digital customer interfaces technically demanding and sometimes requiring bespoke middleware development that exceeds internal technical capacity. Mamede et al. (2023) identified analogous patterns in their study of Portuguese banking RPA adoption, noting that institutions that invested in process standardization and technical infrastructure rationalization before deploying new technology systems achieved substantially better integration outcomes than those that attempted to overlay new tools on unrestructured legacy environments.

Table 7.
Key Technical Issues Impacting Technology Deployment (N = 42)

Technical Issue	n	(%)
Data quality and integrity	6	14.3
System compatibility	25	59.5
Scalability	4	9.5
Security vulnerabilities	7	16.7



Security vulnerabilities, identified by 16.7% of respondents, rank second among technical concerns – a position that understates the institution-level strategic salience of cybersecurity risk, which respondents identify as the foremost long-term risk. This apparent discrepancy reflects a distinction between technical implementation challenges (where system compatibility dominates) and long-term institutional risk (where security dominates): security vulnerabilities may not be the primary obstacle to getting a system deployed, but they constitute the most consequential risk once deployment has occurred.

Vendor Technical Support Quality

The vendor support quality ratings are predominantly positive, with 83.3% of respondents rating support as good, very good, or excellent. Only 16.7% rate support as fair or poor. This finding is instructive in the context of the broader adoption challenge picture: the relative adequacy of vendor technical support, set against the demonstrated deficits in internal technical capacity, suggests that the most productive institutional strategy for technology adoption in resource-constrained NBFCs may be to leverage vendor capabilities more intensively rather than attempting to internalize technical competencies whose development would require sustained investment in human capital over longer time horizons. The finding should, however, be interpreted with awareness of a potential satisfaction bias: vendor support that appears adequate for current deployment challenges may prove insufficient as institutions advance to more complex implementations requiring deeper customization and integration.

Table 8.
Rating of Technical Support Provided by Technology Vendors (N = 42)

Rating	n	(%)
Excellent	4	9.5
Very Good	14	33.3
Good	17	40.5
Fair	6	14.3
Poor	1	2.4



Technology Aspects Requiring Improvement

System integration requirements for improvement (52.4%) are consistent with the dominance of system compatibility as the primary technical implementation obstacle identified in Table 7. The convergence of these two findings strengthens the conclusion that integration capability – both in terms of the technical standards to which vendor products adhere and the quality of integration tools they provide – is the single most commercially actionable improvement priority for technology vendors serving the NBFC segment. Data processing speed (23.8%) reflects performance constraints that may be particularly acute for institutions deploying AI models whose inference latency affects customer-facing application response times, and for those whose legacy hardware infrastructure does not support the computational demands of modern machine learning workloads.

Table 9.

Technology Aspects Requiring Improvement for Better Implementation (N = 42)

Improvement Area	n	(%)
User interface	7	16.7
System integration	22	52.4
Data processing speed	10	23.8
Security features	3	7.1

Most Noticeable Long-Term Technology Benefits

Operational efficiency gains are identified as the most noticeable long-term technology benefit by 52.4% of respondents – a finding that aligns with the primary motivation for RPA adoption documented in the literature and with the measurable cost reductions of 30%–70% that empirical studies of banking RPA implementations have documented (Jangir et al., 2024). Enhanced decision-making (23.8%) captures the contribution of AI-based credit scoring and risk assessment systems, whose most direct institutional value lies in improving the accuracy of lending decisions and reducing non-performing asset ratios – an outcome with both commercial and regulatory significance for NBFCs operating under increasing scrutiny of their credit portfolio quality. Customer service improvement (16.7%) likely reflects the impact of



chatbot and digital communication platforms that have reduced customer query response times and enabled asynchronous service delivery across time zones.

Table 10.

Most Noticeable Long-Term Benefits of Adopting New Technologies (N = 42)

Benefit Category	n	(%)
Improved customer service	7	16.7
Operational efficiency gains	22	52.4
Enhanced decision-making	10	23.8
Improved security outcomes	3	7.1

Metrics for Measuring Long-Term Technology Implementation Success

User satisfaction emerges as the primary long-term success metric for technology implementations among the sampled institutions (52.4%), followed by operational metrics (23.8%) and financial performance (19.0%). The prominence of user satisfaction as a success criterion reflects the fundamentally customer-facing character of NBFC technology deployment: the primary channel through which technology adoption generates institutional value is through improvements in the customer experience – faster loan approvals, more accessible digital onboarding,

Table 11.

Metrics for Measuring Long-Term Success of Technology Implementations (N = 42)

Success Metric	n	(%)
Financial performance	7	19.0
User satisfaction	22	52.4
Operational metrics	10	23.8
Compliance with regulations	3	4.8



more responsive service interfaces – rather than through internally visible efficiency improvements that remain opaque to customers. This customer-centric success framing also suggests that NBFCs may be underweighting the internal efficiency and financial performance dimensions of technology ROI in their institutional evaluation frameworks, potentially leading to underinvestment in back-office automation relative to customer-facing digital interface development.

Greatest Long-Term Risks Associated with Technology Adoption

The risk distribution in Table 12 is among the most concentrated findings in the survey: 71.4% of respondents identify data security breaches as the greatest long-term technology adoption risk – a consensus that is both substantively appropriate and empirically grounded in India's evolving cybersecurity threat landscape. The national data are unambiguous on this point: CERT-In documented 4,29,847 cybersecurity incidents targeting financial institutions in 2023 (PwC India, 2024), Indian financial enterprises experienced an average data breach cost of USD 2.35 million in 2024 (Fintech News Singapore, 2025), and the Digital Threat Report 2024 identified AI-powered attacks, ransomware, and third-party vendor vulnerabilities as the dominant and intensifying threat vectors (CERT-In, CSIRT-Fin & SISA, 2024). For smaller NBFCs operating with resource-constrained security functions, the risk of a material breach is not merely financial but existential: the reputational consequences of a disclosed breach affecting customer financial and identity data in an environment of heightened regulatory scrutiny under the Digital Personal Data Protection Act, 2023, could compromise the institution's commercial viability in ways that far exceed

Table 12.

Greatest Long-Term Risks Associated with New Technology Adoption (N = 42)

Long-Term Risk	n	(%)
Rapid technological obsolescence	6	14.3
Data security breaches	30	71.4
Increased operational complexity	4	9.5
Regulatory non-compliance	2	4.8



the direct cost of the breach itself. Technological obsolescence (14.3%), the second most frequently identified risk, reflects the pace of change in the AI and automation technology landscape, in which solutions adopted today may require significant reinvestment within three to five years to maintain competitive functionality.

Areas Requiring Additional Practical Guidance

Implementation strategy (38.1%) and training and support (35.7%) are identified as the two areas most urgently requiring additional practical guidance, with a combined 73.8% of respondents prioritizing these dimensions over technology selection and post-implementation review. This distribution is theoretically significant: technology selection is a bounded, point-in-time decision that occurs once per technology adoption cycle, whilst implementation strategy and training are sustained, iterative institutional investments that determine whether the selected technology actually delivers its promised benefits. The finding that NBFCs most urgently need guidance on how to implement technology effectively – and how to build the workforce capacity to operate it sustainably – rather than on which technology to choose, implies that the primary bottleneck is institutional and organizational rather than informational. Industry associations, regulatory sandboxes, and peer learning networks may be better positioned than conventional technology consultancy to address the implementation strategy and training guidance gaps identified here.

Table 13.

Areas That Would Benefit Most from Additional Practical Guidance (N = 42)

Guidance Area	n	(%)
Technology selection	9	21.4
Implementation strategy	16	38.1
Training and support	15	35.7
Post-implementation review	2	4.8



Adequacy of Available Guidance for Technology Implementation

The modal response of 'Somewhat adequate' (38.1%), followed closely by 'Neutral' (35.7%), describes a guidance landscape that respondents regard as passable rather than satisfactory. Taken together, the finding that 21.5% rate available guidance as inadequate or very inadequate, whilst only 42.9% rate it as adequate or very adequate, indicates a meaningful institutional demand for better structured, more contextually relevant technology implementation guidance. The gap may be particularly acute for guidance on the intersection of technology implementation and regulatory compliance – an area where generic technology deployment advice and generic regulatory compliance guidance both exist in abundance, but where the specific challenges of managing a technology implementation whilst simultaneously satisfying evolving regulatory requirements are addressed by comparatively little practically accessible institutional guidance.

Table 14.

Adequacy of Available Guidance for Implementing New Technologies (N = 42)

Guidance Adequacy	n	(%)
Very adequate	2	4.8
Somewhat adequate	16	38.1
Neutral	15	35.7
Somewhat inadequate	7	16.7
Very inadequate	2	4.8

CONCLUSIONS AND RECOMMENDATIONS

This study has examined the technology adoption landscape of Non-Banking Financial Companies registered in Guwahati, Assam, generating primary empirical evidence on the challenges, operational experiences, and perceived risks and benefits associated with the integration of AI, RPA, and cybersecurity systems. The findings reveal an institution-level technology adoption environment characterized by five analytically distinct features: a workforce capability gap that constitutes the primary



structural barrier to adoption; a legacy system integration challenge that is pervasive and tractable but not currently well-supported by vendor or institutional investment; a regulatory environment that is dynamically evolving and frequently impactful but perceived by most institutions as navigable rather than prohibitive; a cybersecurity risk profile that is broadly and correctly recognized as the foremost long-term institutional vulnerability; and a benefit realization pattern centered on operational efficiency and decision-making improvement that confirms the instrumental case for technology adoption despite the institutional costs involved.

The following strategic recommendations flow directly from the empirical findings.

1. Given that workforce skill deficits constitute the primary adoption barrier, NBFCs should pursue talent development through channels that are accessible at their institutional scale. Industry association-led training programs, partnerships with regional technical universities and management institutions, and participation in government-sponsored skilling initiatives – such as those supported by the National Skill Development Corporation – offer pathways to AI, RPA, and cybersecurity capability development that avoid the prohibitive cost of full-time specialized hiring. Regulatory sandbox participation through the RBI's Innovation Hub provides an additional avenue for smaller NBFCs to develop digital capabilities with institutional support.

2. Given that system compatibility is the dominant technical obstacle and system integration the most frequently cited area requiring improvement, technology investment priorities should include middleware solutions and API-layer investments that improve the interoperability of existing core systems with new technology platforms. The Lean-before-RPA approach demonstrated by Mamede et al. (2023) – standardizing and simplifying existing processes before automating them – is particularly relevant for institutions where process complexity and inconsistency would undermine the effectiveness of direct RPA deployment.

3. The finding that 71.4% of respondents identify data security breaches as the foremost long-term technology risk, set against the national evidence that cybersecurity threats targeting India's financial sector intensified dramatically between 2019 and 2024, makes a compelling institutional case for treating cybersecurity investment as a strategic priority rather than a compliance line item. Practical measures appropriate to NBFC scale include multi-factor authentication as baseline access control, encrypted data storage and transmission for all customer financial and identity data, incident response planning and testing, and vendor security assessment as a standard procurement requirement.



4. Given that 41.8% of respondents report regulatory changes often or always affecting their technology implementation, the institutional design of technology adoption programs must incorporate regulatory monitoring as a first-order function, with dedicated responsibility for tracking RBI, SEBI, and data protection regulatory developments and translating their implications into technology roadmap adjustments. External legal and regulatory advisory relationships offer cost-effective access to regulatory expertise for institutions whose internal compliance functions are not resourced for proactive regulatory intelligence.

5. The finding that user satisfaction dominates institutional success metrics, with operational and financial performance metrics receiving comparatively less weight, suggests that NBFCs may be underinvesting in the back-office automation and operational efficiency applications that typically generate the highest measurable financial returns from technology investment. Establishing formal productivity and return-on-investment tracking systems for technology implementations would provide the institutional evidence base needed to justify continued investment and to identify underperforming deployments early.

LIMITATIONS AND DIRECTIONS FOR FUTURE RESEARCH

This study is subject to several limitations that should inform both the interpretation of its findings and the design of subsequent research. The sample is restricted to 40 NBFCs in a single northeastern Indian city, and the findings cannot be generalized to the full national population of NBFCs, which encompasses institutions of significantly greater scale, technological maturity, and regulatory complexity operating in metropolitan financial centers. The descriptive correlational design does not permit causal inference about the relationships between technology adoption investments and institutional outcomes. Self-reported survey responses are subject to social desirability bias and may not accurately reflect actual institutional practices, particularly regarding sensitive topics such as cybersecurity incidents and regulatory compliance failures.

Future research should pursue at least three analytical extensions. First, comparative studies contrasting NBFC technology adoption dynamics across geographic tiers – metropolitan, Tier-2, and Tier-3 city contexts – would provide the institutional differentiation necessary to tailor policy and capacity-building recommendations to the heterogeneous population of Indian NBFCs. Second, longitudinal studies tracking the same institutions across multiple years would enable the examination of adoption trajectories and the lagged performance effects of technology investments that a single cross-sectional survey cannot capture. Third, qualitative investigations using in-depth interviews with technology and compliance



leadership within NBFCs would provide the explanatory depth — on the decision processes, institutional politics, and external relationships that shape technology adoption choices — that survey instruments are structurally unsuited to deliver.

REFERENCES

- Ahmed, S. S. (2024). Analyzing the non-banking financial institutions in Bangladesh: A comparative analysis with IDLC Finance PLC. *International Journal of Finance and Accounting*, 13(2), 45–62.
- CERT-In, CSIRT-Fin, & SISA. (2024). *Digital Threat Report 2024: India's BFSI sector*. Government of India, Ministry of Electronics and Information Technology.
- Chen, Y., Wu, H., & Zhang, L. (2023). Artificial intelligence and financial innovation: Implications for financial markets. *Technological Forecasting and Social Change*, 188, Article 122278. <https://doi.org/10.1016/j.techfore.2022.122278>
- Edunjobi, T. E., & Odejide, O. A. (2024). Theoretical frameworks in AI for credit risk assessment: Towards banking efficiency and accuracy. *International Journal of Scientific Research Updates*, 7(1), 92–102. <https://doi.org/10.53430/ijrsru.2024.7.1.0048>
- Elets BFSI. (2024, September). *The rise of NBFCs in the digital age*. <https://bfsi.eletsonline.com/the-rise-of-nbfc-in-the-digital-age/>
- Elets BFSI. (2026). *Cyber resilience in the age of AI: How India's NBFCs can stay ahead of evolving threats*. <https://bfsi.eletsonline.com/cyber-resilience-in-the-age-of-ai-how-indias-nbfc-can-stay-ahead-of-evolving-threats/>
- Fintech News Singapore. (2025, May). *Cyber threats surge in India's financial sector*. <https://fintechnews.sg/110964/fintech-india/cyber-threats-surge-in-indias-financial-sector/>
- Jangir, K., Sharma, V., Gupta, M., Sharma, P., & Pathak, N. (2024). Role of increase in efficiency in adoption of robotic process automation in non-banking financial companies. *AIP Conference Proceedings*, 2919(1). AIP Publishing. <https://doi.org/10.1063/5.0182793>
- Kaur, H. (2019). Growth trend of non-banking finance companies. *Think India Journal*, 22(4), 10491–10497.
- Khan, S. D. (2023). A systematic approach on customer relationship management practices in non-banking companies. *Journal of Informatics Education and Research*, 3(2). <https://doi.org/10.52783/jier.v3i2.222>



Loutfi, A. A. (2022). A framework for evaluating the business deployability of digital footprint-based models for consumer credit. *Journal of Business Research*, 152, 473–486. <https://doi.org/10.1016/j.jbusres.2022.07.042>

Mamede, H. S., Gonçalves Martins, C. M., & Mira da Silva, M. (2023). Lean RPA: Integrating lean process improvement with robotic process automation. In W. van der Aalst et al. (Eds.), *Lecture Notes in Business Information Processing: Business Process Management Workshops* (pp. 297–314). Springer. <https://doi.org/10.1002/9781394166954.ch20>

Manukyan, H., & Parsyan, S. (2024). Customer credit worthiness in the digital age: A management approach to machine learning application in banking. *Proceedings on Engineering Sciences*, 6(2), 665–672. <https://doi.org/10.24874/PES06.02.017>

PwC India. (2024). *Beyond the cloud: Navigating FinTech cyber threats and fortifying defences*. PricewaterhouseCoopers India. <https://www.pwc.in/assets/pdfs/consulting/beyond-the-cloud-navigating-fintech-cyber-threats-and-fortifying-defences-v3.pdf>

Rai, A., Sharma, N., & Gupta, V. (2023). A study on financial technology and cyber security in India. *International Scientific Journal of Engineering and Management*, 2(4). <https://doi.org/10.55041/ISJEM00350>

Reserve Bank of India. (2023). *Master Direction on Information Technology Governance, Risk, Controls, and Assurance Practices*. <https://www.rbi.org.in>

Sengupta, R., Son, L. L., & Vardhan, H. (2022). *A study of the non-banking finance companies in India*. Indira Gandhi Institute of Development Research Working Paper.

Shah, S. R. (2023). An impact study of role of NBFCs: New path of development of MSME business in India. *International Journal of Commerce and Management Studies*, 8(1), 1–12. <https://doi.org/10.56843/IJCOMS-2456-3684>